An Enhanced Remote User Authentication Scheme with Smart Card

Manoj Kumar
Department of Mathematics, Rashtriya Kishan College
Meerut- Karnal Road Shamli-247776, District-Muzaffarnagar, Utter Pradesh-India
(Email: {yamu_balyan@yahoo.co.in)
(Received June 29, 2008; revised Oct. 27, 2008; and accepted Mar. 25, 2009)

Abstract

In 2000, Hwang and Li's proposed a new remote user authentication scheme with smart cards. Some researchers pointed out the security weaknesses of Hwang and Li's scheme and they also proposed some modified schemes to avoid these weaknesses. In 2004, Kumar proposed a new remote user authentication scheme and try to solve the security problems of Hwang and Li's scheme. This paper analyzes that Kumar's scheme does not satisfy some essential security requirements. Kumar's scheme does not support mutual authentication, session key generation phase for secure communication. In addition, in Kumar's scheme, the remote user is not free to change his password. This paper present an enhanced remote user authentication scheme with smart card that not only resolves all the security problems of Hwang and Li's scheme, but also adds mutual authentication, session key generation and password change phase to Kumar's scheme and provides forward secrecy to the long term secret key of the remote server. In the proposed scheme, first the server and user authenticate one another and then generate a secret session key for secure communication. In our scheme, the remote user is free to change his/her password without connecting to server.

Keywords: Cryptology, electronic authentication, network security, password, smart card

1 Introduction

Communicating securely through open networks is one of the common necessity. To solve this problem, remote user authentication scheme [6, 37, 29] is one of the simplest and the most convenient authentication mechanism to deal with secret data over insecure networks. These types of schemes are applicable to the areas such as computer networks, wireless networks, remote login systems, operation systems, and database management systems. The primary goal of a remote user authentication scheme is to identify a valid card holder as having the rights and privileges indicated by the issuer of the card. Thus, smart card based remote user authentication schemes are widely acknowledged as one of the most secure and reliable forms of electronic identification. With the help of remote user authentication schemes, people can interact with the sever through distributed or portable terminals. In a remote user authentication scheme, the authenticity and integrity of the user and the server are important elements over an insecure network. At their best, the remote user and remote server can securely authenticate each other, processing and protecting the communication in a convenient and user friendly manner. At the worst, some security vulnerabilities can be there. Actually, a password based remote user authentication scheme consists three components: remote user, remote server and an secure/insecure channel to connect them. A typical smart card based remote user authentication scheme comprises three phases: registration phase, login phase and authentication phase. In the registration phase, a user U sends a registration request to remote server AS and submits some necessary and unique information to the server through a secure channel. The server uses these information: user's identity and password along with its long-term secret to generate some values and stores some of them in a smart card, which then delivered to the user. In the login phase, a user attaches his smart card to a smart card reader and keys in his identity and password to login the server to gain access right. The smart card then uses the password and the values in the card to construct a login request and then sends it to the remote server. In the authentication phase, the server uses its long-term secret to check the validity of the login request. If mutual authentication is required, the server also uses its long-term secret to construct a message and sends it back to the user. The user then uses his password and the values in the smart card to check the validity of the message. In mutual authentication, the remote server and remote user not only authenticate one another, but also generate a secure session key. In recent years, so many remote user authentication schemes with smart cards [4, 5, 7, 11, 12, 14, 16, 18, 20, 22, 23, 28, 31, 32, 33] have been proposed to authenticate a legitimate user, but

none of them can solve all possible problems and withstand all possible attacks [30]. Thus, at this stage, We are concerned with mutual authentication and secure session generation. For security point of view, it is better to consider these topics jointly rather than separately. A protocol providing authentication without key exchange is susceptible to an enemy who waits until the authentication is complete and then takes over one end of the communications line. Such an attack is not precluded by a key exchange that is independent of authentication. Key exchange should be linked to mutual authentication so that a party has assurances that an exchanged key (which might be used to facilitate privacy or integrity and thus keep authenticity alive) is in fact shared with the authenticated party, and not an impostor. For these reasons, it is essential to keep key exchange abe mutual authentication in mind in the design and analysis of authentication protocols.

1.1 Related Work

In 1981, Lamport [19] proposed the first well-known remote password authentication scheme using smart cards. In Lamport's scheme, the AS stores a password table at the server to check the validity of the login request made by the user. However, high hash overhead and the necessity for password resetting decrease the suitability and practical ability of Lamport's scheme. In addition, the Lamport scheme is vulnerable to a small n attack [26]. Since then, many similar schemes [13, 21, 34] have proposed. They all have a common feature: a verification password table should be securely stored in the AS. Actually, this property is a disadvantage for the security point of view. The AS will be partially or totally braked/affected, If the adversary stolen, removed, or modified the password table. In 2000, Hwang and Li [15] pointed that Lamport's scheme suffers from the risk of a modified password table and the cost of protecting and maintaining the password table. Further, they proposed a new remote user authentication scheme using smart cards. Hwang and Li's [15] scheme does not maintain the password table at the server to check the validity of the login request. Also, it can withstand message-replaying attack [35]. In 2000, Chan and Cheng [2] pointed out the security weakness of Hwang-Li's scheme [15]. In 2003, Shen-Lin-Hwang [27] discussed a different type of attack on the Hwang-Li's scheme and they also proposed a modified scheme to solve the security problem of Hwang-Li's scheme. In the same year, Chang and Hwang [3] explained the practical problems of the Chan-Cheng's attack [2] on the Hwang-Li's scheme and Leung, Cheng, Fong and Chen [22] pointed out that the Shen-Lin-Hwang's scheme [27] is still vulnerable to the attack proposed by Chan and Cheng [2]. Awasthi and Lal [1] pointed out a different type of attack on Hwang-Li's scheme and they introduced a remote user authentication scheme. Awasthi and Lal [1] claimed that their scheme provides forward secrecy to the AS. In 2004, Kumar [25] analyzed the practical pitfalls of Awasthi and Lal 's scheme [1]. In the same year, Lee et al. [20] raised a question on the correctness of Awasthi and Lal's scheme [1]. Lee et al. [20] also proved that Awasthi and Lal's scheme [1] is incorrect and does not provide the forward secrecy to the secret key of the authentication server AS. In 2004, Kumar [24] proposed a new scheme to solve the security problems of Hwang-Li's scheme [15], Kumar' scheme [24] solved the securities problems of Hwang-Li's scheme [15], but does not provide complete solution to solve all the possible problems and withstand all possible attacks.

1.2 Contribution

Kumar's scheme [24] does not support the following three most essential security requirements:

1) Remote user is not free to change his password.

2) This scheme does not support session key generation.

3) The scheme does not support mutual authentication.

Keeping in mind all the these requirements,this paper presents an enhanced remote user authentication scheme that not only resolves all the security problems of Hwang and Li's scheme [15], but also provides mutual authentication, session key generation and password change phase to Kumar's scheme [24]. The proposed scheme not only resolves all the security problems of Hwang and Li's scheme [15], but also provides essential security requirements for secure communication. The proposed scheme also provides forward secrecy with respect to the long - term secret key of the AS, if compromised of the secret key of the AS does not result in compromise of the security of the previously registered identities and the corresponding passwords.The proposed scheme enables the remote user to change his password freely and securely without the help of remote server. In addition, our scheme also provides mutual authentication and session key generation for secure communication between U and AS.

1.3 Organization

The remainder of this paper is organized as follows. Section 2 is about the notations. Section 3 reviews the Kumar's scheme [24]. Section 4 presents an enhanced remote user authentication scheme with smart card. The security of the proposed scheme is analyzed in Section 5. Section 6 is about the attributes of the proposed scheme. The proposed scheme is compared with Hwang-Li's scheme [15] and its varients [1, 24, 27] in Section 7. Finally, comes to conclusion in the Section 8.

2 Notations

The notations used through out this paper are summarized as follows:

- U denotes a remote user.

- ID denotes an identity of a remote user U.
- PW denotes a password corresponding to a registered identity ID.
- AS denotes an authentication server.
- x_s denotes a permanent secret key of an authentication server.
- $f(\cdot)$ denotes a cryptographic one way hash function.
- $\oplus$ denotes the bitwise XOR operation.
- $U \Longleftrightarrow AS$: M User U sends M to the server AS through a secret channel.
- $U \Longrightarrow AS$: M denotes that user U sends M to the server AS through an open channel.
- p denotes a large prime number.
- S_{ID} denotes the redirected identity corresponding to a registered identity ID.
- C_{ID} denotes a check digit sum corresponding to a registered identity ID [8, 9, 10].
- $Red(\cdot)$ denotes a function to redirect the identity ID for every user U, which is only possessed with the AS.
- $C_K(\cdot)$ denotes a function to generate check digit for the registered identity [8, 9, 10], which is only possessed with the AS.

3 Review of Kumar's Scheme

There are three phases in the Kumar's scheme [24]: the registration phase, login phase and the authentication phase. In the registration phase, the user U sends a request to the AS for the registration. The AS will issue a smart card and a password to every user legal through a secure channel. In the login Phase, when the user U wants to access the AS, she/he inserts her/his smart card to the smart card reader and then keys the identity and the password to access services. In the authentication phase, the AS checks the validity of the login request.

3.1 Registration Phase

In the registration phase, user U submits a string J to AS, consists the name of the user U, address, identity ID and a unique identification number etc, which are unique for the user U. AS computes $S_{ID} = Red(J), C_{ID} = C_K(S_{ID}), PW = (S_{ID})^{x_s} \bmod p$. AS delivers $(S_{ID} \| C_{ID}, PW)$ and a smart card to the user U through a secure channel. The smart card contains the public parameters (f, p).

3.2 Login Phase

User U attaches her/his smart card to the smart card reader and keys identity ($S_{ID} \| C_{ID}$ and PW. The smart card will perform the following operations:

1) Generate a random number r.
2) Compute $C_1 = (S_{ID})^r \bmod p$.
3) Compute $t = f(T \oplus PW) \bmod p - 1$, where T is the current date and time of the smart card reader.
4) Compute $M = (S_{ID})^t \bmod p$.
5) Compute $C_2 = M(PW)^r \bmod p$.
6) Sends a login request $C = (S_{ID} \| C_{ID}, C_1, C_2, T)$ to the AS.

3.3 Authentication Phase

Assume AS receives the message C at time T_c, where T_c is the current date and time at AS. Then the AS takes the following actions:

1) Check the format of S_{ID}. If the format is not correct, then AS will rejects this login request.
2) Check, whether $T_c - T \leq \Delta T$, where ΔT is the legal time interval due to transmission delay, if not, then rejects the login request C.
3) Compute $PW = (S_{ID})^{x_s} \bmod p$ and $t = f(T \oplus PW) \bmod (p-1)$.
4) Check, if $C_2 = C_1^{x_s}(S_{ID})^t \bmod p$, then the AS accepts the login request. Otherwise, the login request will be rejected.

Thus, we can say that Kumar's scheme [24] does not support mutual authentication and session key generation. In Kumar's scheme [24] the remote user is not free to change his password.

4 An Enhanced Remote User Authentication Scheme with Smart Card

This section presents an enhanced remote user authentication scheme smart card. This scheme has four phases: registration phase, login phase and verification phase and password change phase. In the registration phase, the remote user registered herself/himself at the server by providing some personal and unique information over a secure channel. On the basis of these information, the remote server computes some parameters related to the user and stored some of them in the smart card and then handed over this smart card to user. The login phase provides the facility of a secure login to the user. The

user has to entered *PIN* (Personal Identification Number) to active the smart card. The concept of *PUK* (Personal Unblocking Key) [17] code is introduced in the login phase to enhanced the security of the login phase. In the verification phase, the server checked the validity of the login request made by the remote user and then the server and user also authenticate one another. In our scheme, not only the server authenticate the remote user but the remote user also authenticate the remote server. After mutual authentication, a secure session key is generated for secure communication. In the password change phase, the remote user is free to change her/his password without connecting to the remote server. Thus, the proposed scheme not only resolves all the security problems of Hwang and Li's scheme [15], but also provides essential security requirements for secure communication.

On the other end, the secret key of the *AS* is a long-term key. It means the secret key of the server requires further security. Consider the situation, when the secret key of the *AS* is revealed or compromised by an accident or stolen etc, then it is not better to replace/alter the whole system at the *AS*. It is also not efficient to replace/alter the secret key of the *AS* with the previously registered identities and their corresponding passwords. However, the secret key of the *AS* requires further security in term of forward secrecy: the revelation or publication of the secret key of the *AS* does not result in compromise of the security of the previously registered identities and their corresponding passwords. The proposed scheme provides forward secrecy to the *AS*. Forward secrecy ensures that the previously generated identities and their corresponding passwords in the *AS* are secure even if the systems secret key x_s has been revealed or known publicly by an accident or is stolen by any adversary etc. For our requirement, we have modified the Hwang and Li's scheme [15]. This proposed scheme uses two more functions: redirected function $Red(\cdot)$ to redirect the registered identity *ID* and a check digit function $C_K(\cdot)$ [8, 9, 10] to generates the corresponding check digit [8, 9, 10] for each registered identity. In this scheme, only the *AS* can redirect the registered identity *ID* and then generate a valid identity and the corresponding check digit [8, 9, 10]. The proposed scheme is described below.

4.1 Registration Phase

This phase is invoked whenever a user U wants to register himself at the remote server *AS*. This phase is executed over a secure channel. The following steps are involved in this phase.

Step R_1. $U \Longleftrightarrow AS$: J
The string J is the registration request, consists the name of the user U, address, identity *ID* and a unique identification number etc, which are unique for the user U.

Step R_2. Upon receiving the registration request, the *AS* computes the followings parameters: $S_{ID} = Red(ID), C_{ID} = C_K(S_{ID}), PW = (S_{ID})^{x_s} \bmod p$ and $R = S_{ID} \oplus PW$.

Step R_3. $AS \Longleftrightarrow U$: $(ID \| C_{ID}, PW)$ and a smart card. In the proposed scheme, the smart card of a user U contains the parameters *f*, *p*, $f(S_{ID})$ and R.

4.2 The Login Phase

Whenever, the user wants to gain the access right on the *AS*, U attaches her/his smart card to the smart card reader at any time T and keys in the *PIN* (Personal Identification Number) to active the smart card. If the *PIN* code is entered incorrectly multiple times, the smart card may request a *PUK* (Personal Unblocking Key) code [17]. Inputs her/his identity $ID \| C_{ID}$ and the corresponding password PW. The smart card of the user U conducts the following computations:

Step L_1. Compute $S_{ID} = R \oplus PW$, $f(S_{ID})$ and compare the calculated $f(S_{ID})$ and stored $f(S_{ID})$, if they are equal the smart card accept the password PW and proceeds to the next step, otherwise demands the password again.

Step L_2. Generate a random number r and compute $C_1 = (R \oplus S_{ID})^r \bmod p$.

Step L_3. Compute $t = f(T \oplus PW) \bmod p - 1$, where T is the current date and time of the smart card reader.

Step L_4. Compute $M = (S_{ID})^t \bmod p$ and compute $C_2 = M(PW)^r \bmod p$.

Step L_5. $U \Longrightarrow AS$: $L_R = (ID \| C_{ID}, C_1, C_2, R, T)$.

4.3 The Verification Phase

Assume that the *AS* receives the login request L_R at time T_c. Then, *AS* does the following computations to check the validity of the login request L_R.

Step V_1. Check the specific format of the identity *ID*. If the format of the identity is incorrect, then *AS* rejects the login request L_R.

Step V_2. Computes the value $S_{ID} = Red(ID)$. Check, whether the condition $C_{ID} = C_K(S_{ID})$ holds, if not, then *AS* rejects the login request L_R.

Step V_3. Check, whether $T_c - T \leq \Delta T_S$, where ΔT_S is the legal time interval due to transmission delay, if not, then *AS* rejects the login request L_R.

Step V_4. Compute $PW = R \oplus S_{ID}$ and $t = f(T \oplus PW) \bmod p - 1$, and check, if $C_2 = (C_1^{x_s})(S_{ID})^t \bmod p$, then the *AS* accepts the login request and proceeds to the next step. Otherwise the login request will be rejected by *AS*.

Step V_5. The AS selects a random number r_1 and computes the following values:

$$C_3 = f(C_1^{x_s} \oplus T_S),$$

where T_S is the current time at AS.

$$\begin{aligned} S_{key} &= f(C_1^{x_s}, T_S, r_1), \\ C_4 &= C_3 \oplus r_1, \\ C_5 &= C_3 \oplus S_{key}. \end{aligned}$$

Step V_6. $AS \Longrightarrow U$: (C_4, C_5, T_S).

Step V_7. Assume that the U receives the message (C_4, C_5, T_S) at time T_U, then U verifies, whether $\mathrm{T}_U - T_S \leq \Delta T_U$, where ΔT_U is the legal time interval due to transmission delay, if not, then U interrupts the connection. The smart card performs the following steps.

1) Computes $C_3^* = f(C_2 M^{-1} \oplus T_S)$.
2) Computes $r^* = C_3^* \oplus C_4$.
3) Computes $S_{key}^* = C_3^* \oplus C_5$.
4) Computes $S_{key}^{**} = f(C_2 M^{-1}, T_S, r^*)$.
5) Compares S_{key}^* and S_{key}^{**} for mutual authentication, if they are equal the user U ensures that the responding system is a real AS and proceeds to the next step. Otherwise U interrupts the connection. The number S_{key}^* will be the session key between the user U and AS,

Step V_8. U computes $C_6 = f(C_3^*, S_{key}^*)$. $U \Longrightarrow AS$: (ID, C_6).

Step V_9. AS checks, if $C_6 = f(C_3, S_{key})$, then the AS assures that the user U also generates the same session key, otherwise rejects the connection.

4.4 The Password Change Phase

This phase is invoked whenever U wants to change his password PW with a new password, say $PWnew$. This phase has the following steps.

Step P_1. U inserts her/his smart card to the smart card reader and then keys in the PIN to active the smart card,then inputs her/his identity and the old password PW and then requests to change the password.

Step P_2. Compute $S_{ID} = R \oplus PW$, $f(S_{ID})$ and compare the calculated $f(S_{ID})$ and stored $f(S_{ID})$, if they are equal the smart card accept the password change request and proceeds to the next step, otherwise demands the correct the password again.

Step P_3. U's smart cards computes $R^* = R \oplus PW \oplus PW_{new}$ and then replaces R with R^*.

5 Security Discussion

Secure mutual authentication and secret session key generation are two important pillars, which are responsible for the security of a remote user authentication scheme. In other words, a remote user authentication scheme is secure if each user can get an authenticated secret session key after performing the secure mutual authentication protocol and all other users can learn nothing about that session key. This section is about the security of the proposed scheme. The proposed protocol provides explicit key authentication, mutual authentication. The proposed scheme resists the replay attack [35], stolen verifier attack [4], password guessing attack, smart card lost attack, parallel session attack,impersonation attack, attack via identity, attack via password. The proposed scheme is also forward secure, which means if the the secret key of the AS compromised then security of the previously registered identities and the corresponding passwords will not be compromised.

SR1: Explicit Key Authentication

Let U and AS be two honest terminals who execute the steps of an authentication protocol correctly,then an authentication scheme provides the explicit key authentication, if it should satisfy following two properties [17]:

- **Implicit key authentication** - Informally speaking, an authentication protocol is said to provide implicit key authentication (of AS to U) if entity U is assumed that no other entity from a specifically identified second entity AS can possibly learn the value of the particular secret key.
- **Key confirmation** - an authentication protocol is said to provide key confirmation (of AS to U) if entity U is assumed that second entity AS actually possession of a particular secret key.

Observe Steps V_5 to V_7 of verification phase of the proposed scheme. These steps show that only the specified user and specified server can get correct information which can be used to generate a valid session key. This means that the proposed scheme provides implicit key authentication. In Step V_7, the server AS assures the user had computed the same session.

SR2: Replay Attack

When the adversary impersonates a legal user to login the specified server by replaying [35] the transmitted messages between the legal user and that server, then we say that this protocol is vulnerable to the replay attack [35]. Suppose that an adversary collects the messages $L_R = (ID \| C_{ID}, C_1, C_2, T)$ from Step L_5, (C_4, C_5, T_S) from Step V_6 and (ID, C_6) from Step V_8 of the proposed protocol. The adversary impersonates the user U to login the server AS by replying the message $\mathrm{L}_R = (ID \| C_{ID}, C_1, C_2, T)$. The

Step V_3 of the verification phase does not satisfy, due to the invalid time interval. It is clear that the adversary can not select a valid time T to avoid this invalid transmission delay. Thus, the server will detect that he/she is not a valid user U. Also, the adversary can not generate the correct (C_4, C_5, T_S) corresponding to r_1 and returns it to the user U because he does not know the secret key of the server AS. In this case, the user U will detect the fabricated server with the help of Step V_7. In the same way, the Step V_9 will detect the replaying of the message (ID, C_6). Hence, it is very hard for an adversary to masquerade the legal user to login the server by replaying the old message.

SR3: Stolen-verifier Attacks
An attacker who steals the password-verifier (e.g., hashed passwords) from the server can use the stolen-verifier [4] to impersonate a legal user to login to the system. The proposed scheme is free from the stolen verifier attack [4]. There is no such information stored at the server, by which an adversary can make a fabricated login request to impersonate a legal user to login the server, or can impersonate the server to cheat the legal user.

SR4: Forward Secrecy
Forward secrecy ensures that the previously generated passwords in the system are secure even if the system secret key x_s has been revealed in public by accident or is stolen. Take a look on the registration phase of our scheme. With a secret key x_s, the AS uses two additional functions: $Red(\cdot)$ and $C_K(\cdot)$, which are always in possession of AS. In this way, only the AS is able to compute a redirected/ shadowed identity SID and a check digit sum C_{ID} corresponding to every valid identity ID. Unfortunately, if the secret key x_s of the AS is revealed or compromised by an accident or stolen etc, then with the help of revealed secret key x_s any attacker Bob can try to obtain the password PW corresponding to the previously registered identity string J/ID or he can try to generate new password by selecting a newly valid identity string J_{new}. Thus, he can try to obtain some fake passwords. But, when he tries to obtain the password PW corresponding to a previously registered ID or the password corresponding to a newly selected valid identity string J_{new} , he is required to compute a redirected/ shadowed identity S_{ID} and a check digit sum C_{ID} [8, 9, 10] corresponding to every valid identity string J, whether it is old or new. Without the knowledge of corresponding shadowed identity S_{ID} and a check digit sum C_{ID} [8, 9, 10] for a identity ID, the attacker will not be able to recover a valid pair of proper identity and the proper corresponding password to make a valid login request. The login request does not leak any information for the attacker, while the attacker is in possession of the secret key of the AS. Thus, our scheme provides forward secrecy with respect to the long - term secret key x_s of the AS if compromised of the secret key of the AS does not result in compromise of the security of the previously registered identities and the corresponding passwords.

SR5: Denial of Service Attacks
In this attack, the attacker can update false verification information of a legal user for the next login phase. Afterwards, the legal user will not be able to login successfully anymore. Since no secret information of the remote user is stored at the server, therefore the attacker will not able to form this type of changes.

SR6: Forgery Attacks (Impersonation Attacks)
In this attack, an attacker attempts to modify intercepted communications to masquerade the legal user and login to the system. In our scheme,the attacker can intercept the login request $L_R = (ID \| C_{ID}, C_1, C_2, R, T)$, $(C_4, C_5, T_S$ and (ID, C_6). But due to the inclusion of time stamp T and T_S in these intercepted information, the attacker will not be able to masquerade the legal user.

SR7: Mutual Authentication
In Kumar's scheme [24] only the remote server check the validity of the login request and authenticate the remote server and the remote user is not sure that he/she logged on a valid remote server. Thus, there is a possibility of server spoofing attack where an attacker pretends to be the server to manipulate sensitive data of the legal users. There is also no session key generation phase in Kumar's scheme [24]. Thus, we are concerned with mutual authentication and secure session generation. Already, we have described that why it is better to consider mutual authentication and session key generation jointly rather than separately. Observe Steps V_5 to V_9 of the verification phase of the proposed scheme, which are responsible for mutual authentication secure session key generation. Thus, in our scheme, not only the server authenticate the legal users, but the user also check the authenticity of the legal server and then generate a secure session key for each fresh session.

SR8: Parallel Session Attack
In parallel session attack, without knowing a user password, an attacker can masquerade as the legal user by creating a valid login message out of some eavesdropped communication between the user and the server. In our scheme,the attacker can intercept the login request $L_R = (ID \| C_{ID}, C_1, C_2, R, T)$, (C_4, C_5, T_S) and (ID, C_6). But due to the inclusion of time stamp T and T_S in these intercepted information, the attacker will not able to masquerade the legal user.

SR9: Password Guessing Attacks
Most passwords have such low entropy that it is vul-

nerable to password guessing attacks, where an attacker intercepts authentication messages and stores them locally and then attempts to use a guessed password to verifies the correctness of his/her guess using theses authentication messages. In our scheme, the attacker can intercept the login request $L_R = (ID\|C_{ID}, C_1, C_2, R, T)$, (C_4, C_5, T_S) and (ID, C_6) and stores them locally and then tries to find out a password to verifies the correctness of his/her guess using theses authentication messages. On observing these pieces of information, we can say that the proposed in free from the password guessing attack because these information are generated either with discrete logarithm or XOR, which are computationally infeasible.

SR10: Smart Card Loss Attacks
When the smart card is lost or stolen, unauthorized users can easily change the password of the smart card, or can guess the password of the user by using password guessing attacks, or can impersonate the user to login to the system. In our scheme, when the attacker wants to change the password of the stolen smart card, the Personal Identification Number is required to active the smart card, which is in possession of smart card owner. If the PIN code is entered incorrectly multiple times, the smart card may request a *PUK* (Personal Unblocking Key) code [17] and the smart card will be seized/blocked.

SR11: Attack Via Registered Identity
In Shen-Lin-Hwang's attack [27], the attacker Bob is not a registered user at the *AS*. To create some favorable results for a successful attack, he requires the redirected identity S_{ID} of a previously registered user, say Alice. But in our scheme, the redirected identity S_{ID} of every registered user is calculated secretly by the *AS* with the help of $Red(\cdot)$ function. The function $Red(\cdot)$ redirects a valid identity into a shadow identity S_{ID} on the basis of the information, which is sent by the user at the time of registration request. *AS* computes the password by using the $PW = (S_{ID})^{x_s} \bmod p$, where S_{ID} a redirected secret value corresponding to the registered identity *ID* of the string *J*. Assume that an eavesdropper, Bob intercepts the login request $L_R = (ID\|C_{ID}, C_1, C_2, R, T)$ from a public network, then it is clear that by using the login request L_R neither he can obtain any information to attack the scheme nor he can compute the password *PW* from this login request L_R. In our scheme, there is no way for the attacker to register herself/himself by intercepting the login request L_R. He is not able to produce any fabricated results for a successful attack. Consequently, the functionality of $Red(\cdot)$ blocks the masquerade attack via identity: Shen-Lin-Hwang's attack [27].

SR12: Attack Via Password
In Chan-Cheng's attack [2] and Chang-Hwang's Attack [3], the attacker Alice is a registered user at the *AS*. To create some fabricated results for a successful attack, only he has the knowledge of a secret redirected identity S_{ID} corresponding to her registered identity *ID*. To perform Chan-Cheng's attack [2] and Chang-Hwang's attack [3], the attacker Alice computes $S_{ID_B} = (S_{ID_A})^k \bmod p$, where k is a random number. Then, he can compute the corresponding password $PW_B = (PW_A)^k \bmod p$. This result is incomplete; still, it is essential to obtain the corresponding check digit of S_{ID_B}. In our scheme, only the *AS* can generate a valid check digit [8, 9, 10] corresponding to the redirected identity S_{ID_B}. As a result, a legal user Alice cannot compute a valid pair of identity and password to impersonate other user Bob to gain the access login right at the *AS*. Thus, Chang-Hwang's attack [3] will not work. Since, Chan -Cheng's attack [2] is another form of this attack, so this attack also will not work. Consequently, the functionality of $C_K(\cdot)$ blocks the attacks via password - Cheng's attack/Chang-Hwang's attack [3].

6 Attributes of the Proposed Scheme

This section is about the attributes of the proposed scheme.

Attributes A_1:
In the proposed scheme, the password table, verification tables or any other secret information of the remote user are not stored at the remote server. This attribute blocks the possibility of denial of Service Attacks. It means in our scheme attacker can not update false verification information of a legal user for the next login phase.

Attributes A_2:
The proposed scheme has a password change phase. In the proposed scheme, the remote user is free to change her/his password without connecting to the server. In our scheme, only the authorized remote user is able to change her/his password.

Attributes A_3:
Since, there is no role of the remote server in password change phase, therefore in our scheme the remote user is able to set a new password, which cannot be revealed by the administrator of the server.

Attributes A_4:
In our scheme,any unauthorized login can be quickly detected when a user inputs a wrong password. Whenever the smart card is inserted into the smart card reader, it demands Personal Identification Number to active the smart card, which is in possession of smart card owner. If the PIN code is entered incorrectly multiple times, the smart card may request

a *PUK* (Personal Unblocking Key) code [17] and the smart card will be seized/blocked.

Attributes A_5:
In our scheme, the verification phase is a combination of mutual authentication and generation of a secure session key. A secure and fresh session key is established during the mutual authentication process to provide confidentiality of communication.

Attributes A_6:
The proposed scheme provides forward secrecy to the long term secret key of the server. The system and all the information related to the remote server and remote user are still secure even if the secret key of the server is leaked out or stolen and all the registered identity and password will work properly.

7 Comparisons

In this section, we compare the proposed scheme with the Hwang and Li' scheme [15] and its varients [1, 24, 27]. Awasthi-Lal's Scheme [1], Shen- Lin- Hwang's Scheme [27] and Kumar's Scheme [24] of this category in terms of security requirements satisfied and attributes achieved.

7.1 Security Comparisons

In Tables 1, Hwang-Li's scheme [15] and its variants [1, 24, 27] are compared in terms of security requirements satisfied by them. Hwang-Li's scheme [15] and Shen-Lin-Hwang's Scheme [27] do not provide explicit key authentication, forward secrecy, mutual authentication. Hwang-Li's scheme [15] and Shen-Lin-Hwang's Scheme [27] are also not secure against replay attack, impersonation attack, smart card loss attack, attack via registered identity and attack via registered passwords. Awasthi-Lal's scheme [1] does not provides explicit key authentication, forward secrecy, mutual authentication, while this scheme is secure against replay attack, stolen verifier attack, denial of service attack, impersonation attack, parallel session attack. Kumar's scheme [24] also does not provides explicit key authentication, mutual authentication, while this scheme provides forward secrecy to the remote server. On the other side, our scheme provides explicit key authentication, forward secrecy, mutual authentication and secure against replay attack, stolen verifier attack, denial of service attack,impersonation attack,parallel session attack, password guessing attack described in Section 5. However, we can say that in all respect, our scheme is the best scheme among Hwang-Li's scheme and its variants in terms of security requirements.

7.2 Attributes Comparisons

In Table 2, Hwang-Li's scheme [15] and its variants [1, 24, 27] are compared in terms of attributes archived by them. It is true that in Hwang-Li's scheme and its variants, there is no password verification table is stored at the server but they fail to complete the other attributes. The proposed scheme satisfies all the attributes describes in Section 6. However, we can say that in all respect, our scheme is the best scheme among Hwang-Li's scheme and its variants in terms of attributes.

8 Conclusions

This paper presents an enhanced remote user authentication scheme with smart cards. The proposed scheme not only provides mutual authentication between the user and server, but also establishes a common session key to provide message confidentiality. In addition, the proposed protocol provides the explicit key authentication property for established common session keys. since the secret key of the AS is a long-term key therefore it requires further security. In the situation, when the secret key of the AS is revealed or compromised by an accident or stolen etc, then it is not better to replace/alter the whole system at the AS. It is also not efficient to replace/alter the secret key of the AS with the previously registered identities and their corresponding passwords. However, the secret key of the AS requires further security in term of forward secrecy: the revelation or publication of the secret key of the AS does not result in compromise of the security of the previously registered identities and their corresponding passwords. The proposed scheme also provides forward secrecy to the AS. The proposed protocol is provably secure to withstand the replay attack, the stolen verifier attack , denial of service attack, impersonation attack, parallel session attack, password guessing attack described in Section 5. In the password change phase of the proposed protocol, user can change his password without connecting to any server. Consequently, the proposed scheme adds mutual authentication, session key generation and password change phase to Kumar's scheme and it also overcomes the security vulnerabilities of Hwang and Li's scheme.

References

[1] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smarts cards with forward secrecy," *IEEE Transactions on Consumer Electronic*, vol. 49, no. 4, pp. 1246-1248, 2003.

[2] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronic*, vol. 46, pp. 992-993, 2000.

[3] C. C. Chang and K. F. Hwang, "Some forgery attack on a remote user authentication scheme using smart cards," *Informatics*, vol. 14, no. 3, pp. 189-294, 2003.

[4] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Transactions on Communications*, vol. E85-B, no. 11, pp. 2519-2521, 2002.

Table 1: Security requirement comparisons among the variants of Hwang-Li's scheme

Security Requirements	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9	SR10	SR11	SR12
Hwang-Li's Scheme [15]	No	No	Yes	No	Yes	No	No	No	No	No	No	No
Awasthi-Lal's Scheme [1]	No	Yes	Yes	No	Yes	Yes	No	Yes	No	No	Yes	Yes
Shen-Lin-Hwang's Scheme [27]	No	No	Yes	No	Yes	No	No	No	No	No	No	No
Kumar's Scheme [24]	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes
Our Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2: Attributes comparisons among the variants of Hwang-Li's scheme

Attributes	A1	A2	A3	A4	A5	A6
Hwang-Li's Scheme [15]	Yes	No	No	No	No	No
Awasthi's Scheme [1]	Yes	No	No	No	No	No
Shen-Lin-Hwang's Scheme [27]	Yes	No	No	No	No	No
Kumar's Scheme [24]	Yes	No	No	No	No	Yes
Our Scheme	Yes	Yes	Yes	Yes	Yes	Yes

[5] M. L. Das, A. Saxena, V. P. Gulati and D. B. Phatak, "A novel remote user authentication scheme using bilinear pairings," *Computers and Security*, vol. 25, no. 3, pp. 184-189, 2006.

[6] M. L. Das, "Comments on "Improved efficient rmote user authentication schemes"," *International Journal of Network Security*, vol. 6, no. 3, pp. 282-284, 2008.

[7] G. Fang and G. Huang, "Improvement of recently proposed remote user authentication schemes," *Cryptology ePrint Archive*, 2006. (http://eprint.iacr.org/2006/200.pdf)

[8] J. A. Gallian, "Assigning driver's license number," *Mathematics Magazine*, vol. 64, pp. 13-22, 1991.

[9] J. A. Gallian, "Breaking the Missouri license code," *The UMAP Journal*, vol. 13, pp. 37-42, 1992.

[10] J. A. Gallian and S. Winters, "Modular arithmetic in the marketplace," *The American Mathematical Monthly*, vol. 95, pp. 548-551, 1988.

[11] S. M. Ghanem and H. A. Wahab, "A simple XOR based technique for distributing group key in secure multicasting," *Proceedings of Fifth IEEE Symposium on Computers and Communications (ISCC 2000)*, Antibes, France, pp. 166-171, 3-6 July, 2000.

[12] D. Giri and P. D. Srivastava, "An improved remote user authentication scheme with smart cards using bilinear pairings," *Cryptology ePrint Archive*, 2006. (http://eprint.iacr.org/2006/274.pdf)

[13] D. Giri and P. D. Srivastava, "A cryptographic key assignment scheme for access control in poset ordered hierarchies with enhanced security," *International Journal of Network Security*, vol. 7, no. 2, pp. 223-234, 2008.

[14] C. H. Han and W. K. Shih, "Weaknesses and improvements of the Yoon remote user authentication scheme using smart cards," *Computer Communications*, vol. 32, no. 4, pp. 649-652, 2009.

[15] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronic*, vol. 46, no. 1, pp. 28-30, 2000.

[16] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," *Mathematical and Computer Modeling*, vol. 36, no. 1-2, pp. 103-107, 2002.

[17] IEEE P1363.2-D13, *Standard Specifications for Password-based Public Key Cryptographic Techniques*, IEEE P1363 working group, 2004.

[18] Y. L. Jia, A. M. Zhou, and M. X. Gao, "A new mutual authentication scheme based on nonce and smart cards," *Computer Communications*, vol. 31, no. 10, pp. 2205-2209, 2008.

[19] L. Lamport, "Password authentication with insecure communication," *Communication of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[20] S. W. Lee, H. S. Kim and K. Y. Yoo, "Comment on a remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronic*, vol. 50, no. 2, pp. 576-577, 2004.

[21] R. E. Lennon, S. M. Matyas and C. H. Mayer, "Cryptographic authentication of time-variant quantities," *IEEE Transactions on Consumer Electronic*, vol. 29, no. 6, pp. 773-777, 1981.

[22] K. C. Leung, L. M. Cheng, A. S. Fong and C. K. Chen, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronic*, vol. 49, no. 3, pp. 1243-1245, 2003.

[23] H. T. Liaw, J. F. Lin and W. C. Wu, "An efficient and complete remote user authentication scheme us-

ing smart cards," *Mathematical and Computer Modelling*, vol. 44, pp. 223-228, 2006.
[24] K. Manoj, "New remote user authentication scheme with smart cards," *IEEE Transactions on Consumer Electronic*, vol. 50, no. 2, pp. 597-600, 2004.
[25] K. Manoj, "Some remarks on a remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronic*, vol. 50, no. 2, pp. 615-618, 2004.
[26] C. J. Mitchell and l. Chen, "Comments on the S/KEY user authentication scheme," *ACM Operating System Review*, vol. 30, no. 4, pp. 12-16, 1996.
[27] J. J. Shen, C. W. Lin and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronic*, vol. 49, no. 2, pp. 414-416, 2003.
[28] Z. H. Shen, "A new modified remote user authentication scheme using smart cards," *Applied Mathematics*, vol. 23, no. 3, pp. 371-376, 2008.
[29] X. Tian, R. W. Zhu, D. S. Wong, "Improved efficient remote user authentication schemes," *International Journal of Network Security*, vol. 4, no. 2, pp. 149-154, 2007.
[30] C. S. Tsai, C. C. Lee and M. S. Hwang, "Password authentication schemes: current status and key issues," *International Journal of Network Security*, vol. 3, no. 2, pp. 101-115, 2006.
[31] M. Udi, "A simple scheme to make passwords based on the one-way function much harder to crack," *Computer and Security*, vol. 15, no. 2, pp. 171-176, 1996.
[32] B. Wang and Z. Q. Li, "A forward-secure user authentication scheme with smart cards," *International Journal of Network Security*, vol. 3, no. 2, pp. 116-119, 2006.
[33] R. C. Wang and C. C. Yang, "Cryptanalysis of two improved password authentication schemes using smart cards," *International Journal of Network Security*, vol. 3, no. 3, pp. 283-285, 2006.
[34] Y. Y. Wang, J. Y. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications*, vol. 32, no. 4, PP. 583-585, 2009.
[35] S. M. Yen and K. H. Liao, "Shared authentication token secure against replay and weak key attack," *Information Processing Letters*, vol. 62, no. 2, pp. 77-80, 1997.
[36] C. C. Yang, R. C. Wang, and T. Y. Chang, "An improvement of the Yang-Shieh password authentication schemes," *Applied Mathematics and Computation*, vol. 162, pp. 391-396, 2005.
[37] C. Y. Yang, C. C. Lee, and S. Y. Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object," *International Journal of Network Security*, vol. 1, no. 2, pp. 81-83, 2005.

Manoj Kumar received the B.Sc. degree in mathematics from Meerut University Meerut, in 1993; the M. Sc. in Mathematics (Gold medalist) from C.C.S.University Meerut, in 1995; the M. Phil. (Gold medalist) in Cryptography, from Dr. B. R. A. University Agra, in 1996; the Ph.D. in Cryptography, in 2003. He also qualified the National Eligibility Test (NET), conducted by Council of Scientific and Industrial Research (CSIR), New Delhi-India, in 2000. He also taught applied Mathematics at D. A. V. College, Muzaffarnagar, India from Sep 1999 to March 2001; at S.D. College of Engineering & Technology, Muzaffarnagar- U.P. - INDIA from March 2001 to Nov 2001; at Hindustan College of Science & Technology, Farah, Mathura- U.P. - INDIA, from Nov 2001 to March 2005. In 2005, the Higher Education Commission of U.P. has selected him. Presently, he is working in Department of Mathematics, R. K. College Shamli- Muzaffarnagar-U.P. - INDIA-247776. He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical Science, Ramanujan Mathematical society, and Cryptography Research Society of India. He is working as reviewer for some International peer review Journals: Journal of System and Software, Journal of Computer Security, International Journal of Network Security, The computer networks, computer and security, The Computer Journal. He is also working a Technical Editor for some International peer review Journals- Asian Journal of Mathematics & Statistics, Asian Journal of Algebra, Trends in Applied Sciences Research, Journal of Applied Sciences. He has published his research works at national and international level. His current research interests include Cryptography and Applied Mathematics.